SOME DIVISIBILITY PROPERTIES IN RINGS OF POLYNOMIALS OVER A UNIQUE FACTORIZATION DOMAIN

by

JOSÉ A. VÉLEZ

A thesis submitted in partial fulfillment of the requirements for the degree of

MASTER IN SCIENCE
in
MATHEMATICS

UNIVERSITY OF PUERTO RICO
MAYAGÜEZ CAMPUS
2005

Approved by:

______________________________ _______________
Gabriele Castellini, Ph.D. Date
Member, Graduate Committe

______________________________ _______________
Uroyoán R. Walker-Ramos, Ph.D. Date
Member, Graduate Committe

______________________________ _______________
Luis F. Cáceres, Ph.D. Date
President, Graduate Committe

______________________________ _______________
Wilson Rivera, Ph.D. Date
Representative of Graduate Studies

______________________________ _______________
Pedro Vásquez, Sc.D. Date
Chairperson of the Department

Abstract. Using polynomial evaluation, we give some useful criteria to answer questions about divisibility of polynomials. This allows us to develop interesting results concerning the prime elements in the domain of coefficients of the polynomial. In particular, it is possible to prove that under certain conditions, the domain of coefficients must have infinitely many prime elements. We give alternative characterizations for $D-$rings and present various examples.

Keywords: divisibility properties in ring of polynomials, unique factorization domain, infinite primes property, D-rings.

Resumen. Usando evaluación en polinomios, damos algunos criterios útiles para responder preguntas sobre divisibilidad de polinomios. Esto también permite desarrollar algunos resultados interesantes acerca de los elementos primos del dominio de coeficientes. En particular, es posible demostrar (bajo ciertas condiciones) que el dominio de coeficientes debe tener infinitos elementos primos. Damos también caracterizaciones alternativas de D-anillos y presentamos varios ejemplos.

To my best friend:

Jessika Marie Vázquez.

Acknowledgements

"A man can be happy with any woman as long as he does not love her."
Oscar Wilde - *The Picture of Dorian Gray*

I am grateful to the following people for their support during the course of my graduate studies in Puerto Rico:

Uroyoán Walker, Arturo Portnoy, Gabriele Castellini, Julio Barety, Madeline Ramos, Pedro Alejo Torres, Marggie González, Víctor López and his wife Yolanda, Trilce Encarnación, Ángel Carreras and his wife Ana, Santiago Velasco, Walter Joel Meléndez, Isha Renta, Mario Intrionini, Carlos Santana, Humberto Pérez, Stanislaw Dziobiak, Moisés Delgado, Caroline Rodríguez, Gerardo Hernández and the other graduate students.

I would also like to express my special appreciation to Dr. Pedro Vásquez, Chairman of The Department of Mathematics of The University of Puerto Rico at Mayagüez and his staff for their collaboration.

Special acknowledgement to my friend, boss and advisor Dr. Luis Fernando Cáceres, for his invaluable support and for making my graduate studies be a real dream.

José A. Vélez
Mayagüez, Puerto Rico
May, 2005

Contents

General Introduction

In an Abstract Algebra course, one studies Rings of Polynomials over an integral domain (here simply domain). These rings do satisfy a property called the Division Algorithm. This property allows one to decide if given two polynomials, one divides the other or not. We give divisibility criteria in a ring of polynomials using evaluations with elements in the domain of coefficients. This allows us to develop interesting theories about the prime elements in the domain of coefficients. In particular, it is possible to prove that under certain conditions, the domain of coefficients must have infinitely many primes. In order to develop this investigation it is necessary to approach classical results from Abstract Algebra and therefore, this work serves as a motivation to increase the knowledge about this very important branch of Mathematics.

Briefly, in this document we basically finish closing a certain diagram on some divisibility properties over rings of polynomials in a unique factorization domain, studied by Dr Luis F. Cáceres in his doctoral thesis (see [**3**]).

$$\begin{tikzcd}
IPP \arrow[d, "UFD"'] & DPP \arrow[d, leftrightarrow, "UFD"] \\
SEPP \arrow[r] & EPP
\end{tikzcd}$$

Also, we develop results that are consequences of this equivalence and the definitions of the given divisibility properties.

In Chapter 0, we review basic concepts of Abstract Algebra that are used in the other chapters for readers not familiarized with this topic. Nevertheless, the reader who is proficient in Abstract Algebra can skip this chapter and move directly to Chapter 1. We have assumed the usual notation given to the natural, integer, rational and real numbers. In Chapter 1, the properties of divisibility under our study are defined and we give direct consequences of each one of these definitions. In particular, we are interested in polynomials with integer coefficients. This ring is very interesting, since it fulfills all the given divisibility properties stated in this document. In addition, we prove interesting results about the prime elements in the domain of coefficients. In Chapter 2, we give nontrivial examples that involve the divisibility properties studied in Chapter 1 and concepts from elementary Number Theory.

CHAPTER 0

Fundamentals

1. Commutative rings and unique factorization domains (UFD)

In this chapter we will present some basic definitions and properties from ring theory, specifically from commutative rings theory.

Definition 0.1. Let D be a commutative ring with identity. An element c of D is **irreducible** provided that:

(1) c is a nonzero nonunit;

(2) $c = ab$, with $a, b \in D \Rightarrow a$ or b is a unit.

An element p of D is **prime** provided that:

(1) p is a nonzero nonunit;

(2) $p|ab$, with $a, b \in D \Rightarrow p|a$ or $p|b$.

The set of units of D will be denoted by $D^{\times}$.

Definition 0.2. An integral domain D is a **principal ideal domain** (PID) provided that every ideal $\mathfrak{A}$ of D can be written as $\mathfrak{A} = \langle a \rangle$ for some $a \in D$.

DEFINITION 0.3. An integral domain D is a **unique factorization domain** (UFD) provided that:

(1) every nonzero nonunit element a of D can be written as $a = c_1c_2 \cdots c_n$, with $c_1, ..., c_n$ irreducible elements of D.

(2) If $a = c_1c_2 \cdots c_n$ and $a = d_1d_2 \cdots d_m$ (c_i, d_i irreducible elements of D), then $n = m$ and for some permutation σ of $\{1, 2, ..., n\}$, c_i and $d_{\sigma(i)}$ are associates for every $i = 1, \ldots, n$. This is for each $i = 1, \ldots, n$, there exists a unit u of D such that $c_i = d_{\sigma(i)}u$.

REMARK 0.1. In every UFD irreducible and prime elements coincide.

DEFINITION 0.4. Let $\mathbb{N}$ be the set of non-negative integers and let D be a domain. D is a **Euclidean domain** if there is a function $\phi : D - \{0\} \to \mathbb{N}$ such that:

(1) if $a, b \in D$ and $ab \neq 0$, then $\phi(a) \leq \phi(ab)$;

(2) if $a, b \in D$ and $b \neq 0$, then there exists $q, r \in D$ such that $a = qb + r$ with $r = 0$, or $r \neq 0$ and $\phi(r) < \phi(b)$.

THEOREM 0.1. *Every Euclidean domain D is a PID and every PID is a UFD.*

PROOF. See [**6**, pgs 138-139]. □

DEFINITION 0.5. Let D be a commutative ring. An ideal $\mathfrak{P}$ in D such that $\mathfrak{P} \neq D$ is **prime** if

$$ab \in \mathfrak{P} \Leftrightarrow a \in \mathfrak{P} \text{ or } b \in \mathfrak{P}.$$

DEFINITION 0.6. Let D be a commutative ring. An ideal $\mathfrak{M}$ in D is said to be **maximal** if $\mathfrak{M} \neq D$ and for every ideal $\mathfrak{N}$ such that $\mathfrak{M} \subseteq \mathfrak{N} \subseteq D$, either $\mathfrak{N} = \mathfrak{M}$ or $\mathfrak{N} = D$.

Note that every maximal ideal is also a prime ideal.

LEMMA 0.1. *Every nonunit element of D is contained in a maximal ideal, therefore in a prime ideal as well.*

PROOF. See [**1**, pg 4]. □

PROPOSITION 0.1. *Let D be a domain. Let $\mathfrak{J}(D)$ be the Jacobson Radical of D; this is, $\mathfrak{J}(D)$ is the intersection of all maximal ideals of D. Then, $y \in \mathfrak{J}(D)$ if only if $1 - yx \in D^\times$ for all $x \in D$.*

PROOF. See [**1**, pg 6] or [**7**, pg 51]. □

DEFINITION 0.7. A nonzero element a of a commutative ring D is said to **divide** an element $b \in D$ (notation: $a|b$) if there exists $x \in D$ such that $ax = b$.

DEFINITION 0.8. Let $a_1, ..., a_n$ be elements of a commutative ring D. An element $d \in D$ is the **greatest common divisor** of $a_1, ..., a_n$ (notation: $d = g.c.d.(a_1, ..., a_n)$) provided that:

(1) $d|a_i$ for all $i = 1, ..., n$;

(2) if $c|a_i$ for all $i = 1, ..., n$ with $c \in D$, then $c|d$.

DEFINITION 0.9. Let $a_1, ..., a_n$ be elements of a commutative ring D. An element $m \in D$ is the **least common multiple** of $a_1, ..., a_n$ (notation: $m = l.c.m.(a_1, ..., a_n)$) provided that:

(1) $a_i|m$ for all $i = 1, ..., n$;

(2) if $a_i|c$ for all $i = 1, ..., n$ with $c \in D$, then $m|c$.

LEMMA 0.2. *Let $a_1, ..., a_n$ be elements of a domain D and assume that $d = g.c.d(a_1, ..., a_n)$ exists. Then $m = l.c.m(a_1, ..., a_n)$ exists and moreover:*

$$m = \frac{a_1 \cdots a_n}{d}.$$

THEOREM 0.2. *Let $a_1, ..., a_n$ be elements of a commutative ring D with identity. If D is a UFD, then there exists a greatest common divisor of $a_1, ..., a_n$.*

PROOF. See [**6**, pg 140]. □

COROLLARY 0.1. *Let $a_1, ..., a_n$ be elements of a commutative ring D with identity. If D is a UFD, then there exists a least common multiple of $a_1, ..., a_n$.*

DEFINITION 0.10. Let D be a commutative ring and $D[x]$ be the ring of polynomials with coefficients in D. Let $g(x) \in D[x]$:

(1) if $g(x) = a_n x^n + ... + a_1 x + a_0$ then a $g.c.d.(a_n, ..., a_0)$ is called a **content** of $g(x)$ and is denoted by $C(g(x))$;

(2) if $C(g(x))$ is a unit in D we say that $g(x)$ is **primitive**.

LEMMA 0.3 (Gauss' Lemma). *Let D be a UFD. If $a \in D, f(x), g(x), h(x) \in D[x]$ and $af(x) = g(x)h(x)$, where $g(x)$ is a primitive polynomial, then $h(x) = aq(x)$ for some $q(x) \in D[x]$.*

PROOF. See [**6**, pg 162]. □

The proof of the following Lemmas may be found in [**6**, pgs 157-165].

LEMMA 0.4. *If K is a field, then $K[x]$ is a Euclidean Domain.*

LEMMA 0.5. *If D is a UFD, then $D[x]$ is also a UFD.*

2. Localization

The procedure by which one constructs the rational field $\mathbb{Q}$ from the ring of integers $\mathbb{Z}$ (and embeds $\mathbb{Z}$ in $\mathbb{Q}$) extends easily to any integral domain D and produces the "field of fractions" of D.

DEFINITION 0.11. A non-empty subset S of a ring R is **multiplicative** provided that

$$a, b \in S \Rightarrow ab \in S.$$

THEOREM 0.3. *Let S be a multiplicative subset of a domain D. The relation defined on the set $D \times S$ by*

$$(r, s) \sim (r', s') \Leftrightarrow (rs' - r's) = 0$$

is an equivalence relation.

The equivalence class $(r, s) \in D \times S$ will be denoted by $\frac{r}{s}$, and let $S^{-1}D$ denote the set of equivalence classes. We give a ring structure on $S^{-1}D$ by defining addition and multiplication of these “fractions” $\frac{r}{s}$ in the same way as in elementary algebra: that is,

$$\begin{aligned} \frac{r}{s} + \frac{u}{v} &= \frac{rv + su}{sv} \\ \frac{r}{s}\frac{u}{v} &= \frac{ru}{sv} \end{aligned}$$

The ring $S^{-1}D$ is named as **ring of quotients** of D by S. If S is the set of non-zero elements of D, the ring of quotients $S^{-1}D$ is a field, called the **quotient field** of D and will be denoted as $Q(D)$. Note that $Q(\mathbb{Z}) = \mathbb{Q}$.

If D is commutative ring with identity and $\mathfrak{P}$ a prime ideal of D, then $S - \mathfrak{P}$ is a multiplicative subset of D. The ring of quotients $S^{-1}D = D_{\mathfrak{P}}$ is called the **localization of** D **at** $\mathfrak{P}$.

CHAPTER 1

Definitions

1. Introduction

An interesting question about divisibility is the following: given $f(x)$ and $g(x)$ polynomials with coefficients in the ring of integers $\mathbb{Z}$ such that for all $n \in \mathbb{Z}$, $f(n)|g(n)$, does one have that $f(x)|g(x)$ in $\mathbb{Z}[x]$? Take for example $f(x) = 5$, and $g(x) = x^5 - x$, as a consequence of Fermat's Little Theorem one has that for all $n \in \mathbb{Z}$, $5|n^5 - n$ in $\mathbb{Z}$, but it is not true that $5|x^5 - x$ in $\mathbb{Z}[x]$. However $\mathbb{Z}$ satisfies some properties showing that in many nontrivial cases the answer to that question is affirmative. In order to answer this question, we study some divisibility properties in arbitrary *unique factorization domains* (UFD) : *infinite primes property (IPP), degree polynomial property (DPP), evaluation polynomial property (EPP)* and *strong evaluation polynomial property (SEPP).* These properties give useful tools to understand divisibility in the ring $\mathbb{Z}[x]$ and in any ring of polynomials $D[x]$. Another property that will be useful is the *D-ring* property. In Section 3 we study this property in detail, we give many examples and we prove that in a UFD all these properties are equivalent.

2. Basic definitions

Definition 1.1. An integral domain D satisfies the ***infinite primes property (IPP)*** if given $g(x) \in D[x]$ with $\deg g(x) \geq 1$ the set

$$\{p \in P : (\exists k \in D)(g(k) \neq 0 \text{ and } p|g(k)\}$$

is infinite, where P is the set of primes in D.

It is clear that fields do not satisfy IPP (there are no primes in fields!). It also follows from the definition that rings satisfying the IPP property must contain infinitely many primes.

Example 1.1. Let $g(x) = (x-3)(x+2) \in \mathbb{Z}[x]$. Note that $g(3) = 0$. Let p be a prime such that $p|g(p+3) = p(p+5)$. Note that $\mathbb{Z}$ has infinitely many primes satisfying this condition. Then

$$\{p \in P : (\exists k \in \mathbb{Z})(g(k) \neq 0 \text{ and } p|g(k)\},$$

where P is the set of primes of $\mathbb{Z}$, is infinite.
In general, this set is infinite for any $g(x) \in \mathbb{Z}[x]$ with a root over $\mathbb{Z}$. See proof of Proposition 1.11 below.

Example 1.2. Let p be a prime in $\mathbb{Z}$ such that $p \equiv 1 \mod 4$. It is well-known (see [**4**, pg 151]) that we can find an integer k such that $k^2 + 1 \equiv 0 \mod p$. It is also well-known that the number of primes p such that $p \equiv 1 \mod 4$, is infinite (see [**2**]). Therefore, the set

$$\{p \in P : (\exists k \in \mathbb{Z})(g(k) \neq 0 \text{ and } p|g(k)\},$$

where $g(x) = x^2 + 1$ and P is the set of primes of $\mathbb{Z}$, is infinite.

Example 1.3. Take the polynomial $g(x) = x^2 - 2$. The congruence $x^2 \equiv 2 \mod p$ is solvable if only if $p \equiv 1 \mod 8$. It is well-know that the set of primes having the form

$$p \equiv 1 \mod 8$$

is infinite. Hence the set

$$\{p \in P : (\exists k \in \mathbb{Z})(g(k) \neq 0 \text{ and } p|g(k)\},$$

where $g(x) = x^2 - 2$ and P is the set of primes of $\mathbb{Z}$, is infinite.

We show that the ring of integers $\mathbb{Z}$ satisfies IPP.

Lemma 1.1. *The ring of integers $\mathbb{Z}$ satisfies IPP.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ with $\deg f \geq 1$. Suppose to the contrary that $p_1, p_2, \dots, p_m$ with $p_1 < p_2 < \dots < p_m$ are the only primes of $\mathbb{Z}$ which divide $f(k)$ for any $k \in \mathbb{Z}$ such that $f(k) \neq 0$. Let $f(x) = a_n x^n + \dots + a_1 x + a_0$ and suppose $a_n > 0$. Clearly, $a_0 \neq 0$. Then we can pick l large enough so that ${p_i}^l \nmid a_0 = f(0)$ for $i = 1, \dots, m$. Since $a_n > 0$, we can pick $k > l$ such that ${p_m}^{ml+1} < f({p_1}^k {p_2}^k \cdots {p_m}^k)$, but ${p_1}^k {p_2}^k \cdots {p_m}^k$ is an integer, hence by hypothesis

$$f({p_1}^k {p_2}^k \cdots {p_m}^k) = {p_1}^{j_1} {p_2}^{j_2} \cdots {p_m}^{j_m}, \tag{1}$$

for some $j_1, j_2, \dots, j_m \in \mathbb{Z}^+ \cup \{0\}$.
Note that ${p_1}^{j_1} {p_2}^{j_2} \cdots {p_m}^{j_m} \leq {p_m}^{j_1 + \dots + j_m}$, so $f({p_1}^k {p_2}^k \cdots {p_m}^k) \leq {p_m}^{j_1 + \dots + j_m}$. Hence, ${p_m}^{ml+1} < {p_m}^{j_1 + j_2 + \dots + j_m}$. Therefore $ml+1 < j_1 + j_2 + \dots + j_m$ and so for some i, $l \leq j_i$. Hence by (1), we obtain ${p_i}^l | f({p_1}^k {p_2}^k \cdots {p_m}^k) = a_n({p_1}^k {p_2}^k \cdots {p_m}^k)^n + \dots + a_1({p_1}^k {p_2}^k \cdots {p_m}^k) + a_0$, therefore ${p_i}^l | a_0$. This is a contradiction. □

The following Corollary provides many *principal ideal domains* (PID) satisfying IPP.

Corollary 1.1. *For each $n \in \mathbb{N}$, the ring $\mathbb{Z}\left[\frac{1}{n}\right]$ satisfies IPP.*

Proof. Let $D = \mathbb{Z}\left[\frac{1}{n}\right]$. Let $g(x) \in D[x]$ with $\deg g \geq 1$. There exists $m \in \mathbb{Z}$ such that $mg(x) \in \mathbb{Z}[x]$, then by Lemma 1.1

$$\{p \in P : (\exists k \in \mathbb{Z})(mg(k) \neq 0 \text{ and } p|mg(k)\}$$

is infinite, where P is the set of primes of $\mathbb{Z}$. Therefore

$$\{p \in P : (\exists k \in \mathbb{Z})(g(k) \neq 0 \text{ and } p|g(k)\}$$

is infinite. Hence, if $H = P - \{p \in P : p|n\}$ is the set of primes of D, we obtain that

$$\{p \in H : (\exists k \in D)(g(k) \neq 0 \text{ and } p|g(k)\}$$

is infinite. Therefore D satisfies IPP. □

The following result generalizes the previous Corollary.

Proposition 1.1. *Let D be a UFD and $K = Q(D)$ the quotient field of D. Suppose $D \subseteq S \subseteq K$, where S is a domain, and suppose $dS \subseteq D$ for some nonzero element $d \in D$. Then D satisfies IPP if only if S satisfies IPP.*

Proof. $(\Rightarrow)$ Suppose that D satisfies IPP. Note that $S \subseteq D\left[\frac{1}{d}\right]$. Let $g(x) \in S[x]$ with $\deg g \geq 1$. Because D is a UFD, there exists $m \in D$ with $m \neq 0$ such that $mg(x) \in D[x]$. Moreover, since D satisfies IPP the set

$$\{p \in P : (\exists k \in D)(mg(k) \neq 0 \text{ and } p|mg(k)\}$$

is infinite, where P is the set of primes of D. Therefore

$$\{p \in P : (\exists k \in D)(g(k) \neq 0 \text{ and } p|g(k)\}$$

is infinite. Note that if p is a prime such that $p|d$ then p is a unit of $D\left[\frac{1}{d}\right]$. The primes of $D\left[\frac{1}{d}\right]$ are the primes p in D such that $p \nmid d$. So, the likely primes in S are the primes $p \in P$ such that $p \nmid d$. Hence, if $P - \{p \in P : p|n\} \supseteq H$, where H is the set of primes of S, we obtain that

$$\{p \in H : (\exists k \in S)(g(k) \neq 0 \text{ and } p|g(k)\}$$

is infinite. Therefore S satisfies IPP.

$(\Leftarrow)$ Suppose that S satisfies IPP. Let $f(x) \in D[x]$ with $\deg f \geq 1$. Suppose on the contrary that $p_1, \ldots, p_m$ are the only primes of D which divide $f(k)$, for any $k \in D$ such that $f(k) \neq 0$. Define $g(x) = f(dx)$. Note that $g(x) \in S[x]$ and $\deg g \geq 1$. Let $k \in S$ such that $g(k) \neq 0$. Then $g(k) = f(dk) \neq 0$. Also $dS \subseteq D$, so $dk \in D$. Let p be a prime in S such that $p|g(k)$. Then $p = p_i$ for some $i = 1, \dots, m$ because primes in S are also primes in D. Therefore S does not satisfy IPP and this is a contradiction. □

Definition 1.2. A domain D satisfies ***degree polynomial property (DPP)*** if given $g(x), f(x) \in D[x]$ such that for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$ implies $f(x) = 0$ or $\deg f(x) \geq \deg g(x)$.

There is no field K that satisfies DPP. To see this, take $f(x) = 1$ and $g(x) = x$ in $K[x]$. For all $k \in K$ such that $g(k) \neq 0$ we have that $g(k)|f(k)$ but $f(x) \neq 0$ and $\deg f(x) < \deg g(x)$.

Example 1.4. In Chapter 2, we will show that the ring $\mathbb{Z}[W]$, where

$$W := \{1/p : p \text{ is prime and } p \equiv 1 \mod 4 \text{ or } p = 2\},$$

does not satisfy DPP. Units in this ring are elements $\frac{c}{d}$ with $c \equiv 0 \mod p$ and $p \equiv 1 \mod 4$. Therefore, this ring is not a field.

Lemma 1.2. *Let $g(x), f(x) \in \mathbb{Z}[x]$ such that $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, for $k \in \mathbb{Z}$ arbitrarily large, then $f(x) = 0$ or $\deg f(x) \geq \deg g(x)$.*

Proof. Let $g(x) = a_n x^n + \ldots + a_1 x + a_0$ and $f(x) = b_m x^m + \ldots + b_1 x + b_0$ be polynomials in $\mathbb{Z}[x]$. Without loss of generality suppose $a_n, b_m > 0$. Suppose $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, for $k \in \mathbb{Z}$ arbitrarily large. If $\deg f(x) = m < n = \deg g(x)$ then by elementary calculus we can to find $k \in \mathbb{Z}$ large enough such that $g(k) \neq 0$ and $a_n k^n + \ldots + a_1 k + a_0 > b_m k^m + \ldots + b_1 k + b_0$. This is a contradiction. □

The following result is an immediate consequence of Lemma 1.2.

Corollary 1.2. *The ring $\mathbb{Z}$ satisfies DPP.*

Proposition 1.2. *Let D be a domain. Given $g(y), f(y) \in D[x][y]$ such that $g(x^t)|f(x^t)$, for t arbitrarily large, then $f(y) = 0$ or $\deg_y f(y) \geq \deg_y g(y)$.*

Proof. Let $g(y), f(y) \in D[x][y]$ and suppose $g(x^t)|f(x^t)$ for t arbitrarily large. By $\deg_y f(y)$ we mean the highest exponent of y in $f(y)$. Suppose on the contrary that $f(y) \neq 0$

and $m = \deg_y f(y) < \deg_y g(y) = n$. Let $g(y) = a_n(x)y^n + \ldots + a_1(x)y + a_0(x)$ and $f(y) = b_m(x)y^m + \ldots + b_1(x)y + b_0(x)$. By hypothesis, $g(x^t)|f(x^t)$, for t arbitrary large, therefore if $h(x) = g(x^t) = a_n(x)x^{tn} + \ldots + a_1(x)x^t + a_0(x)$ and $l(x) = f(x^t) = b_m(x)x^{tm} + \ldots + b_1(x)x^t + b_0(x)$ we have $h(x)|l(x)$. Pick t large enough such that $\deg h(x) = \deg(a_n(x) + tn)$ and $\deg l(x) = \deg(b_m(x) + tm)$, $f(x^t) \neq 0$ and $t > \frac{\deg b_m(x) - \deg a_n(x)}{n-m}$, so $\deg h(x) > \deg l(x)$. Since $h(x)|l(x)$, we obtain $l(x) = 0$ or $\deg l(x) \geq \deg h(x)$. In any case, we have a contradiction. Therefore $f(y) = 0$ or $\deg_y f(y) \geq \deg_y g(y)$. □

The next Corollary shows that a ring of polynomials over any domain always satisfies DPP. Its proof follows from Proposition 1.2.

Corollary 1.3. *Let D be an integral domain. The ring of polynomials $D[x]$ satisfies DPP.*

In particular $\mathbb{Z}[x]$ satisfies DPP and using that $D[x][y] = D[x,y]$ one has that $\mathbb{Z}[x_1, ..., x_n]$ satisfies DPP. Furthermore, we have that $K[x_1, \ldots, x_n]$ satisfies DPP for any field K.

Definition 1.3. Let D be a *UFD*. D satisfies ***evaluation polynomial property (EPP)*** if given $f(x), g(x) \in D[x]$ with $g(x)$ primitive, $\deg g(x) \geq 1$ and for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, then $g(x)|f(x)$ in $D[x]$. Of course, this is only true when D is infinite (otherwise D is a field).

There is no infinite field K satisfying EPP. To see that, take $f(x) = 1$ and $g(x) = x$ in $K[x]$. For all $k \in K$ such that $g(k) \neq 0$ we have that $g(k)|f(k)$ but $g(x) \nmid f(x)$. Note for example that for any $k \in \mathbb{Z}$, $5|k^5 - k$ in $\mathbb{Z}$, but $5 \nmid x^5 - x$ in $\mathbb{Z}[x]$.
The following Proposition provides a characterization of the EPP property.

Proposition 1.3. *Let D be a UFD. D satisfies EPP if only if given $f(x)$, $g(x)$ polynomials in $D[x]$ with $g(x)$ irreducible, $\deg g(x) \geq 1$ and for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, then $g(x)|f(x)$ in $D[x]$.*

Proof. See [**3**, pg 30]. □

Now we will see that in a UFD, satisfying DPP is the same that satisfying EPP.

Proposition 1.4. *Let D be a UFD. D satisfies DPP if only if D satisfies EPP*

Proof. Let D be a UFD that satisfies DPP. Let $f(x), g(x) \in D[x]$ with $g(x)$ primitive, $\deg g(x) \geq 1$ and such that for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. Since D satisfies DPP, we obtain $f(x) = 0$ or $\deg f(x) \geq g(x)$. If $f(x) = 0$, we are done. Let $g(x) = a_n x^n + \ldots + a_1 x + a_0$. By the usual Division Algorithm, we can find $s \in D$ and $q(x), r(x) \in D[x]$ such that

$$a_n^s f(x) = g(x)q(x) + r(x) \tag{2}$$

with $\deg r(x) < \deg g(x)$. Since for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, then for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|r(k))$. But D satisfies DPP, so $r(x) = 0$ or $\deg r(x) \geq \deg g(x)$. Hence $r(x) = 0$, then by (2), $g(x)|{a_n}^s f(x)$. Since $g(x)$ is primitive and $\deg g(x) \geq 1$, we obtain by Gauss' Lemma that $g(x)|f(x)$. Therefore D satisfies EPP.

Conversely, suppose D satisfies EPP. Let $f(x), g(x) \in D[x]$ such that for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. If $\deg g(x) \leq 0$, the result is clear. Suppose $\deg g(x) \geq 1$. Then $g(x) = C(g(x))h(x)$ where $C(g(x))$ is the content of $g(x)$ and $h(x)$ is a primitive polynomial in $D[x]$ with $\deg h(x) = \deg g(x)$. By hypothesis, for all $k \in D$, $(h(k) \neq 0 \Rightarrow h(k)|f(k))$. Since D satisfies EPP, $h(x)|f(x)$, then $f(x) = 0$ or $\deg f(x) \geq \deg h(x) = \deg g(x)$. Therefore, D satisfies DPP.

□

By Proposition 1.4 and Corollary 1.2, the proofs of the following Corollaries are immediate.

Corollary 1.4. *The ring $\mathbb{Z}$ satisfies EPP.*

Corollary 1.5. *Let D be a UFD. $D[x]$ satisfies EPP.*

So, by Corollary 1.5, we have in particular that $\mathbb{Z}[x_1, ..., x_n]$ and $K[x_1, \ldots, x_n]$ for any field K, satisfy EPP.

Definition 1.4. Let D be a UFD. D satisfies ***strong evaluation polynomial property*** ($SEPP$) if for each $f(x), g(x) \in D[x]$ where $g(x)$ is irreducible with $\deg g \geq 1$ there exists $I_{g(x)} \subseteq D$ infinite, such that if H is infinite and $H \subseteq I_{g(x)}$, then for all $k \in H$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, implies $g(x)|f(x)$.

Proposition 1.5. *Suppose $f(x), g(x) \in \mathbb{Z}[x]$ with $g(x)$ primitive, $\deg g(x) \geq 1$ and such that $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, for $k \in \mathbb{Z}$ arbitrary large, then $g(x)|f(x)$ in $\mathbb{Z}[x]$.*

Proof. Let $f(x), g(x) \in \mathbb{Z}[x]$ with $g(x)$ primitive, $\deg g(x) \geq 1$ and such that $(g(k) \neq 0 \Rightarrow g(k)|f(k))$, for $k \in \mathbb{Z}$ arbitrary large. By Lemma 1.2 we obtain that $f(x) = 0$ or $\deg f(x) \geq \deg g(x)$. If $f(x) = 0$, we are done. Suppose $\deg f(x) \geq \deg g(x)$ and let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$. By the usual Division Algorithm, we can find $s \in \mathbb{Z}$ and $q(x), r(x) \in \mathbb{Z}[x]$ such that $a_n^s f(x) = g(x)q(x) + r(x)$ with $\deg r(x) < \deg g(x)$. Since $(g(k) \neq 0 \Rightarrow g(k)|f(k))$ for k arbitrary large, then

$$(g(k) \neq 0 \Rightarrow g(k)|r(k)),$$

for k arbitrarily large. By Lemma 1.2, $r(x) = 0$ or $\deg r(x) \geq \deg g(x)$. Therefore $r(x) = 0$. Then $g(x)|a_n^s f(x)$, but $g(x)$ is primitive and $\deg g(x) \geq 1$, so by Gauss' Lemma $g(x)|f(x)$. □

Corollary 1.6. *$\mathbb{Z}$ satisfies $SEPP$.*

Proof. Let $g(x) \in \mathbb{Z}[x]$, irreducible with $\deg g(x) \geq 1$. Let $I_{g(x)} = \mathbb{Z}^+$. Then by Proposition 1.5 we obtain the result. □

The following result provides examples of domains satisfying EPP.

Proposition 1.6. *Let D be a domain. If D satisfies $SEPP$, then D satisfies EPP.*

Proof. Suppose D satisfies $SEPP$. Let $f(x), g(x) \in D[x]$, with $g(x)$ primitive and $\deg g(x) \geq 1$. Suppose that

$$\text{for all } k \in D,\ (g(k) \neq 0 \Rightarrow g(k)|f(k)). \tag{3}$$

Actually, by Proposition 1.3, we can assume that $g(x)$ is irreducible. By hypothesis, there exists $I_{g(x)} \subseteq D$ infinite, such that

$$\text{for each } H \subseteq I_{g(x)} \text{ infinite,} \tag{4}$$

$$\text{if for each } k \in H,\ (g(k) \neq 0 \Rightarrow g(k)|f(k)), \text{ then } g(x)|f(x). \tag{5}$$

By (3) we have that for all $k \in I_{g(x)}$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. In particular, for $H = I_{g(x)}$ in (4), we obtain $g(x)|f(x)$. Therefore D satisfies EPP. □

The following Proposition says that in a UFD, IPP implies $SEPP$. Its proof uses ultraproducts, which is a topic not related to the theory of this document.

PROPOSITION 1.7. *Let D be a UFD. If D satisfies IPP then D satisfies $SEPP$.*

PROOF. See [**3**, pg 36]. □

PROPOSITION 1.8. *Let D be a UFD with at least one prime and with finitely many units, then D satisfies EPP.*

PROOF. See [**3**, pg 38] □

The converse of Proposition 1.8 is not true in general. The ring $\mathbb{Z}\left[\frac{1}{n}\right]$ satisfies EPP by Proposition 1.1, Proposition 1.7 and Proposition 1.6. But it has an infinite number of units. The units of $\mathbb{Z}\left[\frac{1}{n}\right]$ are the integers p^j with p prime and such that $p|n$. However this ring also satisfies DPP and $SEPP$.

3. D-rings

DEFINITION 1.5. Let D be a domain and $K = Q(D)$ its quotient field. D is a ***D*-ring** if given $f(x), g(x) \in D[x]$ such that, if for almost all $k \in D$ (i.e. but a finite number of $k \in D$), $g(k)|f(k)$, then $\frac{f(x)}{g(x)} \in K[x]$

A field is never a D-ring. To see this, let K be a field. Take $f(x) = x$ and $g(x) = 1$, for almost all $k \in D$ we have $f(k)|g(k)$ in K but $\frac{g(x)}{f(x)} \notin Q(K)[x] = K[x]$.

As we will show later, the D-ring property is related with rational functions $r(x)$ over D and polynomials $p(x)$ over K where K its the quotient field of D, such that $r(D)$, $p(D) \subseteq D$. Many interesting results follow from the D-ring property (see [**9**, pgs 61-66] and [**5**]). Our main goal in this section is to show that the D-ring property is equivalent to some of the divisibility properties studied in the previous section.

LEMMA 1.3. *Let $f(x)$ and $g(x) \in \mathbb{Z}[x]$ such that, for almost all $k \in \mathbb{Z}$, $g(k)|f(k)$. Then $\frac{f(x)}{g(x)} \in \mathbb{Q}[x]$, where $\mathbb{Q}$ is the field of rational numbers.*

PROOF. If $g(x)$ is a constant-nonzero polynomial, we are done. Assume $\deg g(x) \geq 1$. Let $A = \{k_1, \ldots, k_n\}$ such that for all $k \in \mathbb{Z} - A$, $g(k)|f(k)$. Let $k_1, \ldots, k_s \in A$ such that $g(k_i) \neq 0$ for $i = 1, \ldots, s$ and let $\beta = g(k_1) \cdots g(k_s)$. If $s = 0$, let $\beta = 1$. Then for all $k \in \mathbb{Z}$ such that $g(k) \neq 0$, $g(k)|\beta f(k)$. Since $\mathbb{Z}$ satisfies EPP we have that $g(x)|\beta f(x)$ in $\mathbb{Z}[x]$. Hence, there exists $p(x) \in \mathbb{Z}[x]$ such that $\beta f(x) = p(x)g(x)$. So $\frac{f(x)}{g(x)} = \beta^{-1}p(x) \in \mathbb{Q}[x]$. □

By Lemma 1.3, we have the following Corollary.

COROLLARY 1.7. *$\mathbb{Z}$ is a D-ring.*

Note that by Corollary 1.7, given $f(x)$ and $g(x)$ polynomials with coefficients in $\mathbb{Z}$ such that $g(k)|f(k)$ implies the existence of a polynomial $h(x) = \frac{f(x)}{g(x)} \in \mathbb{Q}[x]$ with $h(\mathbb{Z}) \subseteq \mathbb{Z}$. For example, for any prime p in $\mathbb{Z}$ we have that for any $k \in \mathbb{Z}$, $p|k^p - k$ which implies that $\frac{x^p - x}{p} \in \mathbb{Q}[x]$.

EXAMPLE 1.5. Consider the ring $\mathbb{Z}[W]$, where

$$W := \{1/p : p \text{ is prime and } p \equiv 1 \mod 4 \text{ or } p = 2\}.$$

We have already shown that this ring is not a field. In Chapter 2, we will show that $\mathbb{Z}[W]$ is not a D-ring either.

DEFINITION 1.6. Let D be a domain. For any polynomial $f(x) \in D[x]$ denote by $S(f)$ the set of all non-zero prime ideals $\mathfrak{P}$ of D such that the congruence $f(x) \equiv 0 \mod \mathfrak{P}$ is solvable in D. This is: there exists $k \in D$ such that $f(k) \in \mathfrak{P}$. In particular, if $c \in D$, $S(c)$ is precisely the set of prime ideals of D that contain c.

PROPOSITION 1.9. *Let D be a domain, K the quotient field of D and $D^{\times}$ the set of units of D . The following properties are equivalent:*

1. *D is a $D-ring$.*
2. *Every polynomial over D which satisfies $f(k) \in D^{\times}$ for almost all $k \in D$ must be a constant.*
3. *For any nonconstant polynomial $f(x) \in D[x]$, the set $S(f)$ is nonempty.*
4. *For any nonconstant polynomial $f(x) \in D[x]$ and any nonzero $c \in D$, the set $S(f) - S(c)$ is infinite.*

PROOF. (1) $\Rightarrow$ (2) If $f(k) \in D^{\times}$ for almost all $k \in D$, then for almost all $k \in D$, $f(k)|1$, thus by (1) $f(x)|1$ in $K[x]$ and so $f(x)$ must be a constant.
(2) $\Rightarrow$ (3) Let f be a non-constant polynomial in $D[x]$. If $S(f)$ is empty, then for every $k \in D$ one has that $f(k) \notin \mathfrak{P}$ for all prime ideal $\mathfrak{P}$ of D. Then for every $k \in D$, $f(k)$ is a unit, otherwise by Lemma 0.1, $f(k)$ is an element of some prime ideal $\mathfrak{P}$, contradicting our hypothesis. So $f(D) \subseteq D^{\times}$, and this is a contradiction.
(3) $\Rightarrow$ (4) Assume $S(f) - S(c)$ to be finite, this is $S(f) - S(c) = \{\mathfrak{P}_1, ..., \mathfrak{P}_n\}$ where $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ are prime ideals of D. Let m be a non-zero element in the ideal $\mathfrak{P}_1\mathfrak{P}_2 \cdots \mathfrak{P}_n$. First consider the $f(0) = 0$ case. In this case for every $k \in D$ one has that $f(k) \in kD$, thus $S(f)$ consists of all prime ideals of D and $S(c)$ contains all but finitely many such ideals. Since $cm \neq 0$ and lies in every prime ideal of D in particular cm lies in every maximal ideal of D, this is $cm \in \mathfrak{J}(D)$. By Lemma 0.1 the polynomial $g(x) = 1 - cmx$ maps D in $D^{\times}$, thus $S(g)$ is empty, contradicting (3).
Now let $f(0) = d \neq 0$. Since all the coefficients of the polynomial $f(cdx)$ are divisible by d, we can write $f(cdx) = dg(x)$ for a suitable polynomial $g \in D[x]$. Since $g(0) = 1$ and the remaining coefficients of $g(x)$ are all divisible by c, then for every $k \in D$ we get $g(k) \equiv 1$ mod $\mathfrak{P}$ for every prime ideal $\mathfrak{P} \in S(c)$. This shows that $S(g)$ and $S(c)$ are disjoint. In view of $S(g) \subseteq S(f)$ we get

$$S(g) \subseteq S(f) - S(c)$$

and it suffices to show the infiniteness of $S(g)$. If $S(g)$ is finite, let b be a non-zero element lying in the product of all members of $S(g)$. Then the polynomial $h(x) = g(bx)$ satisfies

$h(0) = 1$ whereas all the other coefficients are divisible by b. Thus for all $x \in D$ and all prime ideals $\mathfrak{P} \in S(g)$ we have $h(x) \equiv 1 \mod \mathfrak{P}$. But $S(h) \subseteq S(g)$, and so $S(h)$ is empty, contradicting (3).

(4) $\Rightarrow$ (1). Assume that condition (4) holds and that for almost all $k \in D$, $g(k)|f(k)$. Without lost of generalization we may assume that the polynomials f and g are relatively prime in $K[x]$ and thus for suitable polynomials $p, q \in D[x]$ and $c \in D$ we can write

$$p(x)f(x) + q(x)g(x) = c.$$

This shows that for almost all $k \in D$, $g(k)|c$. Assume that $g(x)$ is non-constant. If $\mathfrak{P}$ is a prime ideal belonging to $S(g) - S(c)$, then for some $k \in D$ we have $g(k) \equiv 0 \mod \mathfrak{P}$. Replacing, if necessary, k by a suitable element congruent to $k' \mod \mathfrak{P}$ we may assume that $g(k')|c$, but then c, being a multiple of $g(k')$, would belong to $\mathfrak{P}$, it is a contradiction. Hence g must be constant.

□

Proposition 1.9 gives a very useful tool to prove results about D-rings. The following Corollary gives a characterization of the D-ring property for domains that are not fields, its proof is an immediate consequence of Proposition 1.9.

Corollary 1.8. *Let D be a ring that is not a field and $D^{\times}$ be its set of units. D is not a D-ring if only if there exists a nonconstant polynomial $f(x) \in D[x]$ such that $f(D) \subseteq D^{\times}$.*

The following result gives a relation between a D-ring and its Jacobson Radical.

Proposition 1.10. *Let D be a ring that is not a field. If $\mathfrak{J}(D) \neq (0)$ then D is not a D-ring.*

Proof. If $\mathfrak{J}(D) \neq (0)$, then let $c \in \mathfrak{J}(D)$ with $c \neq 0$. We have that the polynomial $f(x) = 1 - cx$ satisfies $f(D) \subseteq D^{\times}$. By Corollary 1.8, D is not a D-ring. □

There is a relation between *IPP* and the D-ring property. The *IPP* talks about infinitely many prime elements, while the D-ring property talks about infinitely many prime ideals. As a result, in a *PID* it is trivial that *IPP* and the D-ring property are equivalent properties.

Now, we show that any UFD satisfying the D-ring property, also satisfies IPP.

PROPOSITION 1.11. *Let D be a UFD. If D is a D-ring, then D satisfies IPP.*

PROOF. Let $g(x) \in D[x]$ with $\deg g(x) \geq 1$. Suppose that there exists $a \in D$ with $g(a) = 0$. Then, there exists $m \in D$ and $h(x) \in D[x]$ such that $mg(x) = (x-a)h(x)$. Let p be a prime of D such that $p \nmid m$ and $h(p+a) \neq 0$. Note that D has infinitely many primes satisfying this condition. Therefore $mg(p+a) = ph(p+a)$, so $p|mg(p+a)$. By our choice of p, we have that $p|g(p+a)$. Therefore the set

$$\{p \in P : (\exists k \in D)(g(k) \neq 0 \text{ and } p|g(k)\},$$

where P is the set of primes of D is infinite. So, D satisfies IPP.
Suppose that $g(a) \neq 0$ for all $a \in D$. Assume on the contrary that $p_1, \ldots, p_n$ are the only primes of D which divide $g(k)$ for any $k \in D$ such that $g(k) \neq 0$. Let $m = p_1 \cdots p_n$. Since D is a D-ring the set $S(g) - S(m)$ is not empty. Let $\mathfrak{P} \in S(g) - S(m)$, then there exists $k_{\mathfrak{P}} \in D$ such that $g(k_{\mathfrak{P}}) \in \mathfrak{P}$ and $m \notin \mathfrak{P}$. By our assumption

$$g(k_{\mathfrak{P}}) = u{p_1}^{m_1}{p_2}^{m_2} \cdots {p_n}^{m_n},$$

where $u \in D^{\times}$ and m_i is a non-negative integer for $i = 1, \ldots, n$. Since $g(k_{\mathfrak{P}}) \in \mathfrak{P}$, then $u \in \mathfrak{P}$ or there exists $j \in \{1, \ldots, n\}$ such that ${p_j}^{m_j} \in \mathfrak{P}$. If $u \in \mathfrak{P}$ then $\mathfrak{P} = D$ and this contradicts that $\mathfrak{P}$ is a prime ideal of D. If ${p_j}^{m_j} \in \mathfrak{P}$, then $p_j \in \mathfrak{P}$, therefore $m \in \mathfrak{P}$, and this is also a contradiction. Therefore D satisfies IPP. □

The converse of the previous result is also true, but we need some further results in order to prove it. The following Proposition shows that domains that satisfies DPP are D-rings and viceversa.

PROPOSITION 1.12. *Let D be a domain. D is a D-ring if only if D satisfies DPP.*

PROOF. ($\Rightarrow$) Let $g(x), f(x) \in D[x]$ such that for all $k \in D$, $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. So, $g(k)|f(k)$ for almost $k \in D$. Since D is a D-ring, then $\frac{f(x)}{g(x)} \in K[x]$, where K is the quotient field of D. Therefore, there exists $p(x) \in K[x]$ such that $f(x) = p(x)g(x)$. Suppose that

$f(x) \neq 0$, so $\deg f(x) = \deg(p(x)g(x)) = \deg p(x) + \deg g(x) \geq \deg g(x)$, then D satisfies DPP.

($\Leftarrow$) Let $g(x), f(x) \in D[x]$ such that for almost all $k \in D$, $g(k)|f(k)$. Let $A = \{k_1, \ldots, k_n\}$ be a finite subset of D such that $g(k)|f(k)$ for all $k \in D - A$. Let $k_1, \ldots, k_s \in A$ such that $g(k_i) \neq 0$ for $i = 1, \ldots, s$ and let $\beta = g(k_1) \cdots g(k_s)$. If $s = 0$, let $\beta = 1$. Then, for all $k \in D$ such that $g(k) \neq 0$ we obtain that $g(k)|\beta f(k)$. Since D satisfies DPP, then $\beta f(x) = 0$ or $\deg \beta f(x) \geq \deg g(x)$. If $\beta f(x) = 0$, then $f(x) = 0$, so $\frac{f(x)}{g(x)} \in K[x]$. Suppose that $\deg \beta f(x) \geq \deg g(x)$ and assume $g(x) = a_n x^n + \ldots + a_0$ with $a_n \neq 0$. By The Division Algorithm, there exist $q(x), r(x) \in K[x]$ and $s \in D$ such that

$$a_n^s \beta f(x) = g(x)q(x) + r(x),$$

with $r(x) = 0$ or $\deg r(x) < \deg g(x)$ and let $\alpha = a_n^s \beta$. Suppose that $\deg r(x) < \deg g(x)$. Then for all $k \in D$ such that $g(k) \neq 0$ implies that $g(k)|\alpha f(k)$ and $g(k)|g(k)q(k)$. So $g(k)|r(k)$. Hence, using again that D satisfies DPP then $r(x) = 0$ or $\deg r \geq \deg g$. Hence $r(x) = 0$ and we obtain that $\alpha f(x) = g(x)q(x)$. Therefore $\frac{f(x)}{g(x)} = \alpha^{-1} q(x) \in K[x]$. In other words, D is a D-ring. □

The following Proposition shows that $UFD's$ satisfying EPP are D-rings and viceversa.

PROPOSITION 1.13. *Let D be a UFD. D is a D-ring if only if D satisfies EPP.*

PROOF. ($\Rightarrow$) Let $f(x), g(x) \in D[x]$ with g primitive and $\deg(g) \geq 1$ such that for all $k \in D$, $g(k) \neq 0 \Rightarrow g(k)|f(k)$. It is obvious that for almost all $k \in D$, $g(k)|f(k)$. Since D is a $D - ring$ we have that

$$\frac{f(x)}{g(x)} = p(x) \in K[x],$$

where $K = Q(D)$ is the quotient field of D. Let

$$p(x) = \frac{r_n}{s_n} x^n + \frac{r_{n-1}}{s_{n-1}} x^{n-1} + \ldots + \frac{r_1}{s_1} x + \frac{r_0}{s_0},$$

where $r_i, s_i \in D$, with $s_i \neq 0$ for all $i = 0, \ldots, n$. Let $m = l.c.m.(s_n, \ldots, s_0)$, therefore $mp(x) \in D[x]$. Take $h(x) = mp(x)$. Now, we have that

$$mf(x) = mp(x)g(x) = h(x)g(x),$$

with $g(x)$ primitive. By Gauss' Lemma, there exists $q(x) \in D[x]$ such that $h(x) = mq(x)$, and so

$$mf(x) = mq(x)g(x).$$

Therefore we obtain that $f(x) = q(x)g(x)$, with $q(x) \in D[x]$; this is $g(x)|f(x)$ in $D[x]$. In other words, D satisfies EPP.

($\Leftarrow$) Let $f(x), g(x) \in D[x]$ such that for almost all $k \in D$ we have that $g(k)|f(k)$. Let $A = \{k_1, \ldots, k_n\}$ be a finite subset of D such that $g(k)|f(k)$ for all $k \in D - A$. Let $k_1, \ldots, k_s \in A$ such that $g(k_i) \neq 0$ for $i = 1, \ldots, s$ and let $\beta = g(k_1) \cdots g(k_s)$. If $s = 0$, let $\beta = 1$. Then for all $k \in D$ such that $g(k) \neq 0$ we have $g(k)|\beta f(k)$.
Let $K = Q(D)$ be the quotient field of D. We can write $g(x) = \alpha h(x)$ where $h(x)$ is primitive in $D[x]$ with $\deg h = \deg g \geq 1$ and α is the content of $g(x)$. Let $k \in D$ such that $h(k) \neq 0$. Therefore $g(k) \neq 0$ and $g(k)|\beta f(k)$; but $h(k)|g(k)$, so $h(k)|\beta f(k)$. Since D satisfies EPP we have that $h(x)|\beta f(x)$ in $D[x]$. Hence, there exists $p(x) \in D[x]$ such that $\beta f(x) = p(x)h(x)$ and so

$$\alpha\beta f(x) = p(x)(\alpha h(x)) = p(x)g(x),$$

therefore $f(x) = (\alpha\beta)^{-1}p(x)g(x)$ where $(\alpha\beta)^{-1}p(x) \in K[x]$. This is $g(x)|f(x)$ in $K[x]$. In others words, D is a D -ring. □

COROLLARY 1.9. *Let D be a UFD. Then, the ring $D[x]$ is a D-ring.*

PROOF. Immediate from Proposition 1.13 and Corollary 1.5. □

Using the previous Corollary we have that the rings $\mathbb{Z}[x_1, \ldots, x_n]$ and $K[x_1, ..., x_n]$, where K is a field, are D-rings. Note that by Corollary 1.9 and Proposition 1.10, we obtain that for any domain D, $\mathfrak{J}(D[x]) = \{0\}$. Hence, for example, $\mathfrak{J}(\mathbb{Z}[x_1, \ldots, x_n]) = \{0\}$.

The ring $\mathbb{Z}$ satisfies all of our divisibility properties as well as the ring $D[x_1, \dots, x_n]$ for any unique factorization domain D. The following Theorem says that in any UFD, IPP, DPP, EPP, $SEPP$ and D-ring property are equivalent properties.

THEOREM 1.1. *Let D be a UFD. The following properties are equivalent:*

(1) *D is a D-ring.*

(2) *D satisfies IPP.*

(3) *D satisfies $SEPP$.*

(4) *D satisfies EPP.*

(5) *D satisfies DPP.*

PROOF. (1) $\Rightarrow$ (2) from Proposition 1.11, (2) $\Rightarrow$ (3) from Proposition 1.7, (3) $\Rightarrow$ (4) from Proposition 1.6, (4) $\Rightarrow$ (5) from Proposition 1.4 and (5) $\Rightarrow$ (1) from Proposition 1.12. □

We have closed the diagram given in the introduction. Therefore, we have the following diagram where we resume the principal result of this work.

$$\begin{tikzcd}
IPP \arrow[dd, "UFD"'] & & DPP \arrow[dl, leftrightarrow] \arrow[dd, leftrightarrow, "UFD"] \\
& D-ring \arrow[ul, "UFD"'] \arrow[dr, leftrightarrow, "UFD"] & \\
SEPP \arrow[rr] & & EPP
\end{tikzcd}$$

The following Corollary gives infinitely many $PIDs$ that are D-rings. Its proof follows from Proposition 1.1 and Theorem 1.1

COROLLARY 1.10. *For all $n \in \mathbb{N}$, $\mathbb{Z}[\frac{1}{n}]$ is a $D-ring$.*

By Theorem 1.1 and Corollary 1.9 we have that $D[x]$ with D a domain, satisfies all of IPP, DPP, EPP and $SEPP$. Furthermore, $D[x]$ is also a D-ring. Therefore, we have important examples of rings satisfying our divisibility properties, for example: $\mathbb{Z}[x_1, \dots, x_n]$, $\mathbb{Z}_p[x_1, \dots, x_n]$ where p is an integer prime and the ring $\mathbb{R}[x_1, \dots, x_n]$.

Corollary 1.11. *Let D be a UFD and $K = Q(D)$ be the quotient field of D. Suppose $D \subseteq S \subseteq K$, where S is a domain, and suppose $dS \subseteq D$ for some nonzero element $d \in D$. Then D is a D-ring (satisfies DPP, EPP or $SEPP$) if only if S is a D-ring (satisfies DPP, EPP or $SEPP$).*

Proof. Follows directly from Proposition 1.1 and Theorem 1.1. □

We will assume the following results. Proof of these two Propositions may be found in [**5**, pg 299].

Proposition 1.14. *Suppose D is a domain such that $\mathbb{Z} \subseteq D \subseteq \mathbb{Q}$. If D is a non-D-ring, then so is every ring between D and $\mathbb{Q}$. If D is a D-ring, then so is every ring between $\mathbb{Z}$ and D.*

Proposition 1.15. *Among the subdomains of $\mathbb{Q}$ that are infinitely generated over $\mathbb{Z}$, there are infinitely many D-rings and infinitely many non-D-rings.*

In the following example it is necessary to know some results from Algebraic Number Theory, a topic far away from the theory in this document. However, the reader could find more details in [**5**, pg 293].

Example 1.6. Let V be a set of rational primes p such that $\sum_{p \in V} 1/p$ converges. Let U be the set of all p^{-1} $(p \in V)$. Then $S = \mathbb{Z}[U]$ is a D-ring.

Note that $\mathbb{Z}[U]$ is a infinitely generated ring over $\mathbb{Z}$ contained in $\mathbb{Q}$.

4. Infinitely many primes

Proposition 1.16. *Let D be a UFD with at least one prime and finitely many units, then D has infinitely many primes.*

Proof. By Proposition 1.8, D satisfies EPP; therefore D satisfies IPP. Then D has infinitely many primes. □

We give now a direct proof of the previous Proposition. First we prove some Lemmas.

LEMMA 1.4. *Let D be an infinite domain with a finite number of units, then D has an infinite number of maximal ideals.*

PROOF. Suppose that D has a finite number of maximal ideals $\mathfrak{M}_1, ..., \mathfrak{M}_n$. Then the Jacobson Radical of D is $\mathfrak{J}(D) = \bigcap_{k=1}^{n} \mathfrak{M}_k$. Because $\mathfrak{M}_k \neq (0)$ for all $k = 1, ..., n$, then there exists $m_k \in \mathfrak{M}_k$ with $m_k \neq 0$ for each $k = 1, ..., n$. Therefore $m = m_1 \cdots m_n \in \mathfrak{M}_1 \cdots \mathfrak{M}_n \subseteq \mathfrak{J}(D)$ with $m \neq 0$, hence $\mathfrak{J}(D) \neq (0)$. Let $r \in \mathfrak{J}(D)$ with $r \neq 0$, then $1 - r$ is a unit. Let $U = \{u_1, ..., u_s\}$ be the set of units of D, then $r = 1 - u_i$ for some $i = 1, ..., s$; therefore $\mathfrak{J}(D)$ is finite.
Let $x \in \mathfrak{J}(D)$, since $\mathfrak{J}(D)$ is finite then for all $n \geq 1$, there exists $k \leq n$ such that $x^n = x^k$, so $x^{n-k} = 1$, therefore $1 \in \mathfrak{J}(D)$. Then we have that $\mathfrak{J}(D) = D$, so D is finite. This is a contradiction, because D is infinite. □

LEMMA 1.5. *Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n$ be prime ideals of a domain D and let $\mathfrak{A}$ be an ideal of D contained in $\bigcup_{i=1}^{n} \mathfrak{P}_i$. Then $\mathfrak{A} \subseteq \mathfrak{P}_i$ for some i with $i = 1, \ldots, n$.*

PROOF. See [**1**, pg 8].

□

Now we will prove a stronger result than Proposition 1.16. Actually, we could say that the following result is a generalization of Euclid's Theorem about the infinitude of primes.

PROPOSITION 1.17. *Let D be an infinite UFD with a finite number of units, then D has an infinite number of primes.*

PROOF. Suppose $p_1, p_2, \ldots, p_n$ is the whole list of primes in D. Let $D^\times$ be the multiplicative group of D; $\Gamma = \{\langle p_1 \rangle, \ldots, \langle p_n \rangle\}$ and S be the set of all maximal ideals of D. Since D is a UFD we have that

$$D = \langle p_1 \rangle \cup \langle p_2 \rangle \cup \cdots \cup \langle p_n \rangle \cup D^\times.$$

We claim that $S \subseteq \Gamma$. Let $\mathfrak{M} \in S$, then $\mathfrak{M} \subseteq D$. Hence $\mathfrak{M} \subseteq \langle p_1 \rangle \cup \langle p_2 \rangle \cup \cdots \cup \langle p_n \rangle$, where $\langle p_i \rangle$ is a prime ideal of D for $i = 1, \ldots, n$. Then by Lemma 1.5, we have that $\mathfrak{M} \subseteq \langle p_i \rangle$ for some i with $i = 1, \ldots, n$. But $\mathfrak{M}$ is a maximal ideal of D, so $\mathfrak{M} = \langle p_i \rangle$ for some i with

$i = 1, \dots, n$. Then $\mathfrak{M} \in \Gamma$. This proves that $S \subseteq \Gamma$. But Γ is a finite set and by Lemma 1.4, S should be infinite. This is a contradiction. Therefore D has an infinite number of prime elements. □

It is clear that Proposition 1.16 is a direct consequence of Proposition 1.17.

Example 1.7. If $\mathfrak{M}$ is a maximal ideal in a commutative ring D with identity and n is a positive integer, then the ring $D/\mathfrak{M}^n$ has a unique prime ideal and therefore is local. To show this, take the ideal $\mathfrak{M}/\mathfrak{M}^n$ in $D/\mathfrak{M}^n$. Let's show that $\mathfrak{M}/\mathfrak{M}^n$ is prime ideal. Let $(a+\mathfrak{M}^n)(b+\mathfrak{M}^n) \in \mathfrak{M}/\mathfrak{M}^n$, then $ab+\mathfrak{M}^n \in \mathfrak{M}/\mathfrak{M}^n$. So $ab \in \mathfrak{M}$; since $\mathfrak{M}$ is maximal, therefore is prime. Then either $a \in \mathfrak{M}$ or $b \in \mathfrak{M}$, so $a+\mathfrak{M}^n \in \mathfrak{M}/\mathfrak{M}^n$ or $b+\mathfrak{M}^n \in \mathfrak{M}/\mathfrak{M}^n$. This shows that $\mathfrak{M}/\mathfrak{M}^n$ is a prime ideal of $D/\mathfrak{M}^n$. Suppose that $A/\mathfrak{M}^n$ is another prime ideal of $D/\mathfrak{M}^n$, then A is a prime ideal in D such that $\mathfrak{M}^n \subseteq A$. Therefore $\mathfrak{M} \subseteq A$, but $\mathfrak{M}$ is maximal, so $\mathfrak{M} = A$. This proves the uniqueness. By our discussion above, the ring $D = \mathbb{Z}[x]/\langle x, 2\rangle^2$ has a unique prime ideal $\langle x, 2\rangle / \langle x, 2\rangle^2$. Therefore D has finitely many prime elements. This shows that there exists infinite *UFDs* having finitely many prime elements.

By Proposition 1.4 if a domain D is an infinite *PID* with a finite number of units, then D has an infinite number of prime elements.

5. Two variables

The following result shows that one can generalize the divisibility properties to polynomials in many variables. It is sufficient to show the two variables case. The case for any $n \in \mathbb{N}$ results as consequence of the following Proposition.

Proposition 1.18. *Let D be a domain. D satisfies DPP if only if given $f, g \in D[x,y]$ such that for all $a, b \in D$, $(g(a,b) \neq 0 \Rightarrow g(a,b)|f(a,b))$ then $f(x,y) = 0$ or $\deg_y g(x,y) \leq \deg_y f(x,y)$.*
Note that we can replace $\deg_y$ by $\deg_x$.

Proof. ($\Leftarrow$) Since $D[x] \subseteq D[x,y]$ the result it is clear.
($\Rightarrow$) Suppose that $f(x,y) \neq 0$ and $\deg_y g(x,y) > \deg_y f(x,y)$. Let $g(x,y) = c_n(x)y^n + \cdots +$

$c_1(x)y+c_0(x)$ and $f(x,y) = b_m(x)y^m+\cdots+b_1(x)y+b_0(x)$ with $c_n(x), b_m(x) \neq 0$. Note that we would have $\deg_y g(x,y) \geq 1$, because $f(x,y)$ it is a non-zero constant or a non-constant polynomial. Let $a \in D$ such that $c_n(a), b_m(a) \neq 0$. Define $h(y) = g(a,y)$ and $l(y) = f(a,y)$. Note that $\deg_y h(y) = \deg_y g(x,y)$ and $\deg_y l(y) = \deg_y f(x,y)$. Let $b \in D$ such that $h(b) = g(a,b) \neq 0$. By hypothesis, $h(b) = g(a,b)|f(a,b) = l(b)$. Since D satisfies DPP we have that $l(y) = 0$ or $\deg_y h(y) \leq \deg_y l(y)$. If $l(y) = 0$ then $f(a,y) = 0$, contradicting that $f(a,y) \neq 0$. In the other case, if $\deg_y h(y) \leq \deg_y l(y)$ then $\deg_y g(x,y) \leq \deg_y f(x,y)$. This is a contradiction. □

We have the following Corollary from Proposition 1.18.

Corollary 1.12. *Let D be a domain. D satisfies DPP if only if given $f, g \in D[x_1,\ldots,x_n]$ such that for all $a_1,\ldots,a_n \in D$,*

$$g(a_1,\ldots,a_n) \neq 0 \Rightarrow g(a_1,\ldots,a_n)|f(a_1,\ldots,a_n).$$

Then $f(x_1,\ldots,x_n) = 0$ or $\deg_{x_i} g(x_1,\ldots,x_n) \leq \deg_{x_i} f(x_1,\ldots,x_n)$ for all $i = 1,\ldots,n$.

Corollary 1.13. *Let D be a UFD. D satisfies EPP if only if given $f, g \in D[x,y]$, $g(x,y) = g(x)(y)$ primitive with $\deg_y g(x,y) \geq 1$ such that for all $a, b \in D$, $(g(a,b) \neq 0 \Rightarrow g(a,b)|f(a,b))$ then $g(x,y)|f(x,y)$.*

Proof. ($\Leftarrow$) Since $D[x] \subseteq D[x,y]$ the result it is clear.
($\Rightarrow$) Suppose that D satisfies EPP. By Theorem 1.1, D satisfies DPP, then by Proposition 1.18 we have that $f(x,y) = 0$ or $\deg_y g(x,y) \leq \deg_y f(x,y)$. Let $g(x,y) = c_n(x)y^n + \cdots + c_1(x)y + c_0(x)$. By the usual Division Algorithm, we can find $s \in \mathbb{N}$ and $q(x,y), r(x,y) \in D[x,y]$ such that

$$c_n^s(x)f(x,y) = g(x,y)q(x,y) + r(x,y), \qquad (6)$$

with $\deg_y r(x,y) < \deg_y g(x,y)$. Since for all $a, b \in D$ $(g(a,b) \neq 0 \Rightarrow g(a,b)|f(a,b))$, then for all $a, b \in D$ $(g(a,b) \neq 0 \Rightarrow g(a,b)|r(a,b))$. But D satisfies DPP; using the Proposition 1.18 again, we have that $r(x,y) = 0$ or $\deg_y g(x,y) \leq \deg_y g(x,y)$. So $r(x,y) = 0$. By (6), $g(x,y)|c_n^s(x)f(x,y)$. Since $g(x,y)$ is primitive and $\deg_y g(x,y) \geq 1$, by Gauss' Lemma we obtain $g(x,y)|f(x,y)$. □

6. *Int*(D)

DEFINITION 1.7. Let D be a domain and K be its quotient field. The set $Int(D)$ to be the ring of all polynomials $p(x)$ in $K[x]$, such that $p(D) \subseteq D$.

We have that $D[x] \subseteq Int(D) \subseteq K[x]$.
For example: for any prime p, the polynomial $f(x) = \frac{x^p}{p} - \frac{x}{p} \in Int(\mathbb{Z})$ because $f(x) \in \mathbb{Q}[x]$ and $f(\mathbb{Z}) \subseteq \mathbb{Z}$.

DEFINITION 1.8. Let D be a domain. The set $\mathfrak{S}(D)$ is the ring the all rational functions of $D(x)$ such that, given $r(x) \in \mathfrak{S}(D)$, for all $k \in D$ with $k \in dom(r(x))$ implies that $r(k) \in D$.

For example, for $n > 1$, $r(x) = \frac{1-x^n}{1-x} \in \mathfrak{S}(\mathbb{Z})$. In the next Chapter we will give nontrivial examples of polynomials $f(x)$ and $g(x)$ with coefficients in $\mathbb{Z}$ such that for almost all $k \in \mathbb{Z}$, $g(k)|f(k)$ implies $g(x)|f(x)$.
We always have that $Int(D) \subseteq \mathfrak{S}(D)$. But if K is a field $\mathfrak{S}(K) \nsubseteq Int(K)$, because $r(x) = \frac{1}{x} \in \mathfrak{S}(K)$, but $r(x) \notin Int(K)$.
We give an alternative characterization of the divisibility property EPP.

PROPOSITION 1.19. *Let D be a UFD. D satisfies EPP if and only if given $f(x), g(x) \in D[x]$ with* $\deg g \geq 1$ *such that $\frac{f(x)}{g(x)} \in \mathfrak{S}(D)$ then $g(x)|f(x)$ in $D[x]$.*

The following Proposition provides a characterization of D-rings.

PROPOSITION 1.20. *Let D be a domain. D is a D-ring if only if $\mathfrak{S}(D) = Int(D)$.*

PROOF. See [**9**]. □

Note that by Proposition 1.20 and the fact that $\mathbb{Z}$ is a D-ring we have that for any polynomial $h(x) \in \mathbb{Q}[x]$ with $h(\mathbb{Z}) \subseteq \mathbb{Z}$, there exist polynomials $f(x), g(x) \in \mathbb{Z}[x]$ such that $h(x) = \frac{f(x)}{g(x)}$.

EXAMPLE 1.8. There are no localizations $\mathbb{Z}_{\langle p \rangle}$ of $\mathbb{Z}$ with respect to a prime p being D-rings. In fact, define $r(x) = \frac{1}{1+px}$. Let $\alpha \in \mathbb{Z}_{\langle p \rangle}$, then $\alpha = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $b \notin \langle p \rangle$. Then $r(\alpha) = \frac{b}{b+ap}$. It is clear that $b + ap \notin \langle p \rangle$, so $r(\alpha) \in \mathbb{Z}_{\langle p \rangle}$. Therefore $r(x) \in \mathfrak{S}(\mathbb{Z}_{\langle p \rangle})$, but $r(x) \notin Int(\mathbb{Z}_{\langle p \rangle})$. Hence $\mathbb{Z}_{\langle p \rangle}$ is not a D-ring.

CHAPTER 2

Examples

1. Introduction

In the first part of this chapter we will give nontrivial examples of polynomials with coefficients in $\mathbb{Z}$ such that for almost all $k \in \mathbb{Z}$, $g(k)|f(k)$ implies that $g(x)|f(x)$ in $\mathbb{Z}[x]$. In the second part we will show a nontrivial ring generated over $\mathbb{Z}$ contained in $\mathbb{Q}$ that does not satisfy the D-ring property. Finally, we will show that the ring $\mathbb{Z}[\sqrt{d}]$ satisfies DPP, for every $d \in \mathbb{Z}$.

2. The Pell's equation

Consider the following equation:

$$x^2 - dy^2 = 1, \tag{7}$$

where d is an integer that is not a square. This equation is called *Pell's equation.* Lagrange proved that Pell's equation has an infinite number of integer solutions. Furthermore, it is sufficient to find one solution in order to have all of its integer solutions (see [**2**, pg 320]).

We are interested in studying a particular case of Pell's equation:

$$x^2 - (a^2 - 1)y^2 = 1, \tag{8}$$

where $a \in \mathbb{Z} - \{0, -1\}$.

In [**8**] and [**10**, pg 23] the reader may find a proof of the following explicit formula for describing all solutions of (8). These are also known as *Lucas' sequences*:

if $|a| \geq 2$:

$$X_0(a) = 1, \qquad X_1(a) = a, \qquad X_{n+1}(a) = 2aX_n(a) - X_{n-1}(a), \tag{9}$$

$$Y_0(a) = 0, \qquad Y_1(a) = 1, \qquad Y_{n+1}(a) = 2aY_n(a) - Y_{n-1}(a), \tag{10}$$

if $a = 1$, define for all $n \geq 0$:

$$X_n(1) = 1, \tag{11}$$

$$Y_n(1) = n. \tag{12}$$

So, if $|a| \geq 2$ we have:

n	$X_n(a)$	$Y_n(a)$
0	1	0
1	a	1
2	$2a^2 - 1$	$2a$
3	$4a^3 - 3a$	$4a^2 - 1$
4	$8a^4 - 8a^2 + 1$	$8a^3 - 4a$
5	$16a^5 - 20a^3 + 5a$	$16a^4 - 12a^2 + 1$
6	$32a^6 - 48a^4 + 18a^2 - 1$	$32a^5 - 32a^3 + 6a$
7	$64a^7 - 112a^5 + 56a^3 - 7a$	$64a^6 - 80a^4 + 24a^2 - 1$
8	$128a^8 - 256a^6 + 160a^4 - 32a^2 + 1$	$128a^7 - 192a^5 + 80a^3 - 8a$

Note that $X_n(a)$ and $Y_n(a)$ are polynomials in a of degree n and $n - 1$ respectively.

Formula (9) provides an indispensable tool in order to prove the unsolubility of *Hilbert's Tenth Problem.* The following result is known as Julia Robinson's special congruence.

LEMMA 2.1.

$$Y_n(a) \equiv n \mod (a-1), \tag{13}$$

where a and $Y_a(n)$ are as above.

PROOF. See [**10**, pg 26] or [**8**]. □

EXAMPLE 2.1. By (13) we have that for almost all $a \in \mathbb{Z}$, $(a-1)|(Y_n(a)-n)$. Since $\mathbb{Z}$ is a D-ring, then $x-1|Y_n(x)-n$. To have a particular example, take $n=5$, so $Y_5(a) = 16a^4-12a^2+1$, by (13) we have that $a-1|16a^4-12a^2-4$, note that $x-1|16x^4-12x^2-4$.

The following result, proved by Julia Robinson, is useful to show that exponential relations are Diophantine. See [**8**] or [**10**, pg 26].

LEMMA 2.2 (J.Robinson). *For all $k \in \mathbb{N}$ we have:*

$$X_n(a)-(a-k)Y_n(a) \equiv k^n \mod (2ak-k^2-1). \tag{14}$$

EXAMPLE 2.2. Let k be a non-negative integer. By (14) we have that for almost all $a \in \mathbb{Z}$, $2ak-k^2-1|X_n(a)-(a-k)Y_n(a)-k^n$, therefore $2xk-k^2-1|X_n(x)-(x-k)Y_n(x)-k^n$. In particular, if $n=7$ then $X_7(a) = 64a^7-112a^5+56a^3-7a$ and $Y_7(a) = 64a^6-80a^4+24a^2-1$. By (14) we have that

$$\begin{aligned}
2ak-k^2-1|64a^7-112a^5+56a^3-7a-(a-k)64a^6-80a^4+24a^2-1-k^7 \\
&= -32a^5+32a^3-6a+64a^6k-80a^4k+24a^2k-k-k^7 \\
&= (-1+2ak-k^2)(6a-32a^3+32a^5+k-12a^2k \\
&+ 16a^4k-4ak^2+8a^3k^2-k^3+4a^2k^3+2ak^4+k^5).
\end{aligned}$$

and note that

$$2xk-k^2-1|-32x^5+32x^3-6x+64x^6k-80x^4k+24x^2k-k-k^7.$$

The following Lemma (see [**8**] or [**10**, pg 30]) provides a relation between the polynomials $X_n(x)$ and $Y_n(x)$.

LEMMA 2.3.

$$Y_{2n}(a) \equiv 0 \mod X_n(a). \tag{15}$$

EXAMPLE 2.3. By (15), for almost all $a \in \mathbb{Z}$ we have that $X_n(a)|Y_{2n}(a)$; and then

$$X_n(x)|Y_{2n}(x).$$

If $n = 2$, note that for almost all $a \in \mathbb{Z}$ we have that $2a^2 - 1|8a^3 - 4a$, and $2x^2 - 1|8x^3 - 4x$.

The following Lemma provides more relations between $X_n(x)$ and $Y_n(x)$.

LEMMA 2.4. *For $i \geq 1$ we have that:*

$$Y_{4ni\pm m}(a) \equiv \pm Y_m(a) \mod X_n(a), \tag{16}$$

$$Y_{4ni+2n\pm m}(a) \equiv \mp Y_m(a) \mod X_n(a). \tag{17}$$

PROOF. See [**10**, pg 30] or [**8**]. □

EXAMPLE 2.4. Let $i \geq 1$, by Lemma 2.4 for almost all $a \in \mathbb{Z}$ we have that $X_n(a)|Y_{4ni\pm m}(a) \mp Y_m(a)$, therefore $X_n(x)|Y_{4ni\pm m}(x) \mp Y_m(x)$.

3. The ring $\mathbb{Z}[W]$

We assume the following result from Elementary Number Theory.

LEMMA 2.5. *Let p be a prime integer and suppose that for some integer c relatively prime to p we can find integers x and y such that $x^2 + y^2 = cp$. Then p can be written as the sum of squares of two integers, that is, there exists integers a and b such that $p = a^2 + b^2$.*

PROOF. See [**4**, pg 152]. □

THEOREM 2.1 (Fermat). *An odd prime p can be written as $x^2 + y^2$ if only if $p \equiv 1 \mod 4$.*

PROOF. See [**2**, pg 253]. □

EXAMPLE 2.5. Consider the following set

$$W = \{1/p : p \text{ is prime and } p \equiv 1 \mod 4 \text{ or } p = 2\}.$$

We take the ring $S = \mathbb{Z}[W]$ and the polynomial $f(x) = x^2 + 1$, and we will show that $f(S) \subseteq S^{\times}$. Let $\alpha = \frac{a}{b} \in S$. where $a, b \in \mathbb{Z}$ and $g.c.d.(a, b) = 1$. Note that primes that divide b are primes in W. Besides the units in S are elements $\frac{c}{d}$ with $c \equiv 0 \mod p$ and $p \equiv 1 \mod 4$. We have that $f(\alpha) = \frac{a^2+b^2}{b^2}$. Let p_0 be a prime such that $p_0 | a^2 + b^2$, then there exists c such that $a^2 + b^2 = cp_0$. By Lemma 2.5, there exist d and e such that $p_0 = d^2 + e^2$. By Theorem 2.1, $p_0 \equiv 1 \mod 4$. Therefore $f(\alpha) \in S^{\times}$, this is $f(S) \subseteq S^{\times}$. Then, by Proposition 1.8, S is not a D-ring. Consequently, S does not satisfy IPP, DPP, EPP or $SEPP$.

Note that $\mathbb{Z}[W] \subseteq \mathbb{Q}$ is a infinitely generated ring over $\mathbb{Z}$.

4. The ring $\mathbb{Z}[\sqrt{d}]$

Let d be an integer and let $\mathbb{Z}[\sqrt{d}]$ be the subset of complex numbers such that, for every $z \in \mathbb{Z}[\sqrt{d}]$, $z = x + \sqrt{d}y$ with $x, y \in \mathbb{Z}$. Let $z, w \in \mathbb{Z}[\sqrt{d}]$ and assume $z = x + \sqrt{d}y$ and $w = u + \sqrt{d}v$, we can define arithmetic operations over $\mathbb{Z}[\sqrt{d}]$ as follows:

$$z + w = (x + u) + \sqrt{d}(y + v),$$

$$zw = (xu + dyv) + \sqrt{d}(xv + uy).$$

It is easy to see that $\mathbb{Z}[\sqrt{d}]$ with these operations is a domain.

EXAMPLE 2.6. If $d = -1$, the domain $\mathbb{Z}[\sqrt{d}]$ is the *ring of Gaussian Integers* $\mathbb{Z}[i]$. If $d = 2$, we obtain the domain $\mathbb{Z}[\sqrt{2}]$. Note that $\mathbb{Z}[i]$ is an Euclidian Domain, therefore it is a UFD with a finite number of units, it is also an infinite domain. By Proposition 1.17, it has an infinite number a prime elements. The ring $\mathbb{Z}[\sqrt{2}]$ is not a UFD, because there exist prime elements which are not irreducible elements. Moreover, this ring has an infinite number of units. To see this, note that the equation $x^2 - 2y^2 = 1$ has an infinite number of solutions

(x, y) because it is a Pell equation. Therefore, the units of $\mathbb{Z}[\sqrt{d}]$ are the element $x + \sqrt{d}y$ such that $x^2 - dy^2 = 1$. Note that $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$.

This example motivates the following definition.

Definition 2.1. For all $z = x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]$ we define the *conjugate* of z as the complex number $\overline{z} = x - \sqrt{d}y$.

Note that $z = x + \sqrt{d}y \in \mathbb{Z}[\sqrt{d}]$ is a unit if and only if $z\overline{z} = 1$. This is: z is a unit in $\mathbb{Z}[\sqrt{d}]$ if and only if (x, y) is solution of the Pell equation: $x^2 - dy^2 = 1$. Therefore, if $d \geq 2$, the domain $\mathbb{Z}[\sqrt{d}]$ has an infinite number of units. But it is not known in general whether or not $\mathbb{Z}[\sqrt{d}]$ is a UFD.

The following Lemma shows some elementary properties about the conjugate number.

Lemma 2.6. *Let* $z, w \in \mathbb{Z}[\sqrt{d}]$. *Then:*

(1) $z\overline{z} \in \mathbb{Z}$,

(2) $z \in \mathbb{Z}$ *if only if* $\overline{z} = z$,

(3) $\overline{zw} = \overline{z} \cdot \overline{w}$ *and* $\overline{z + w} = \overline{z} + \overline{w}$,

(4) $z\overline{w} + \overline{z}w \in \mathbb{Z}$.

Definition 2.2. Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with $a_0, a_1, \ldots, a_n \in \mathbb{Z}[\sqrt{d}]$. The *conjugate polynomial* $\mathfrak{C}(f)$ of $f(x)$ is the polynomial $\mathfrak{C}(f(x)) = \overline{a_n} x^n + \ldots + \overline{a_1} x + \overline{a_0}$.

Example 2.7. Let $f(x) = (1 - i)x^2 + 3ix + 1$ in $\mathbb{Z}[i][x]$, then $\mathfrak{C}(f(x)) = (1 + i)x^2 - 3ix + 1$.

Example 2.8. Let $f(x) = (1 - \sqrt{2})x^2 - 5x + (4 - 3\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}][x]$, then $\mathfrak{C}(f(x)) = (1 + \sqrt{2})x^2 - 5x + (4 + 3\sqrt{2})$.

In general, note that every polynomial $f(x) \in \mathbb{Z}[\sqrt{d}][x]$ can be written as $f(x) = f_1(x) + \sqrt{d}f_2(x)$, where $f_1(x), f_2(x) \in \mathbb{Z}[x]$. Then $\mathfrak{C}(f(x)) = f_1(x) - \sqrt{d}f_2(x)$. We also have that if $z \in \mathbb{Z}[\sqrt{d}]$, $\mathfrak{C}(z) = \overline{z}$; and for every polynomial $f(x)$ with integer coefficients, $\mathfrak{C}(f(x)) = f(x)$. Conversely, if $\mathfrak{C}(f(x)) = f(x)$ then $f(x)$ is a polynomial with integer coefficients.

The following Proposition shows some elementary properties about the conjugate polynomial.

Proposition 2.1. *Let $f(x), g(x) \in \mathbb{Z}[\sqrt{d}][x]$ and $b \in \mathbb{Z}$. Then:*

(1) $\mathfrak{C}(f(x)+g(x)) = \mathfrak{C}(f(x)) + \mathfrak{C}(g(x))$,

(2) $\mathfrak{C}(f(x)g(x)) = \mathfrak{C}(f(x))\mathfrak{C}(g(x))$,

(3) $\mathfrak{C}(f(b)) = \overline{f(b)}$,

(4) $f(x)\mathfrak{C}(f(x)) \in \mathbb{Z}[x]$,

(5) $f(x)\mathfrak{C}(g(x)) + g(x)\mathfrak{C}(f(x)) \in \mathbb{Z}[x]$.

Definition 2.3. Let $f(x) \in \mathbb{Z}[\sqrt{d}][x]$, we define the *polynomial norm* of $f(x)$ as the polynomial $\boldsymbol{N}(f(x)) = f(x)\mathfrak{C}(f(x))$. Note that $\deg \boldsymbol{N}(f(x)) = 2\deg(f(x))$.

Example 2.9. Let $f(x) = (1-i)x^2 + 3ix + 1$ in $\mathbb{Z}[i][x]$, then $\boldsymbol{N}(f(x)) = [(1-i)x^2 + 3ix + 1][(1+i)x^2 - 3ix + 1] = 2x^4 - 6x^3 + 11x^2 + 1$. Let $g(x) = (1-\sqrt{2})x^2 - 5x + (4-3\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}][x]$, then $\boldsymbol{N}(g(x)) = [(1-\sqrt{2})x^2 - 5x + (4-3\sqrt{2})][(1+\sqrt{2})x^2 - 5x + (4+3\sqrt{2})] = -x^4 - 10x^3 + 21x^2 - 40x - 2$.

Note that in this last example, the polynomials $\boldsymbol{N}(f(x))$ and $\boldsymbol{N}(g(x))$ have integer coefficients. This motivates the following result.

Lemma 2.7. *Let $f(x) \in \mathbb{Z}[\sqrt{d}][x]$. Then:*

(1) *$\boldsymbol{N}(f(x)) = 0$ if and only if $f(x) = 0$,*

(2) *$\boldsymbol{N}(f(x)) \in \mathbb{Z}[x]$,*

(3) *$\boldsymbol{N}(f(x)g(x)) = \boldsymbol{N}(f(x))\boldsymbol{N}(g(x))$,*

(4) *for every $a \in \mathbb{Z}$, $\boldsymbol{N}(f(a)) = f(a)\overline{f(a)}$.*

Proof. Immediate from Lemma 2.1. □

It is already proved in [**9**] and [**5**] that the domain $\mathbb{Z}[\sqrt{d}]$ is a D-ring for every $d \in \mathbb{Z}$. But those proofs are a little complicated and hard to understand. Here, we use the results we have obtained and the above discussion to give a more elementary proof that $\mathbb{Z}[\sqrt{d}]$ satisfies DPP, hence $\mathbb{Z}[\sqrt{d}]$ is a D-ring for every $d \in \mathbb{Z}$.

Proposition 2.2. *For every $d \in \mathbb{Z}$, the ring $\mathbb{Z}[\sqrt{d}]$ satisfies DPP. Therefore, $\mathbb{Z}[\sqrt{d}]$ is a D-ring.*

PROOF. Let $f(x), g(x) \in \mathbb{Z}[\sqrt{d}][x]$ be such that for all $k \in \mathbb{Z}[\sqrt{d}]$ $(g(k) \neq 0 \Rightarrow g(k)|f(k))$. Consider the polynomials with integer coefficients $F(x) = \boldsymbol{N}(f(x))$ and $G(x) = \boldsymbol{N}(g(x))$. Choose $b \in \mathbb{Z}$ such that $G(b) \neq 0$; then $g(b) \neq 0$. By our choice of $g(x)$ we have that $g(b)|f(b)$, and $\overline{g(b)}|\overline{f(b)}$. By elementary divisibility properties, $g(b)\overline{g(b)}|f(b)\overline{f(b)}$. This implies that $G(b)|F(b)$. We had proven that for every $b \in \mathbb{Z}$, $(G(b) \neq 0 \Rightarrow G(b)|F(b))$. Since $\mathbb{Z}$ satisfies DPP, $\deg G(x) \leq \deg F(x)$ or $F(x) = 0$. Hence $\deg g(x) \leq \deg f(x)$ or $f(x) = 0$. In other words, $\mathbb{Z}[\sqrt{d}]$ satisfies DPP. □

COROLLARY 2.1. *For every $d \in \mathbb{Z}$, the ring $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ satisfies DPP. Therefore $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ is a D-ring.*

PROOF. Immediate from Proposition 2.2 and Corollary 1.11. □

Note that the argument used to prove that $\mathbb{Z}[\sqrt{d}]$ satisfies DPP is also useful to prove that $\mathbb{Z}[\sqrt{d_1}, \dots, \sqrt{d_n}]$ satisfies DPP. Therefore, we have the following Corollary.

COROLLARY 2.2. *For every $d_1, \dots, d_n \in \mathbb{Z}$, the ring $\mathbb{Z}[\sqrt{d_1}, \dots, \sqrt{d_n}]$ satisfies DPP. Therefore $\mathbb{Z}[\sqrt{d_1}, \dots, \sqrt{d_n}]$ is a D-ring.*

CHAPTER 3

Conclusions

- The divisibility properties, IPP, DPP, EPP, $SEPP$ and being a D-ring are all equivalent properties in any UFD.
- For every UFD D, the ring of polynomials $D[x]$ satisfies IPP, DPP, EPP and $SEPP$, therefore $D[x]$ is a D-ring as well.
- Every infinite UFD with finitely many units has an infinite number of prime elements.
- For every $d \in \mathbb{Z}$, the domain $\mathbb{Z}[\sqrt{d}]$ satisfies DPP. Therefore, $\mathbb{Z}[\sqrt{d}]$ is a D-ring.

CHAPTER 4

Future Work

The domain of Gaussian Integers $\mathbb{Z}[i]$ is related with the set of primes p, such that p is a sum of squares. Actually, it is proven that this set of primes is infinite. However, there exists a correspondence between these primes and the prime ideals of $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a D-ring, it has infinitely number of prime ideals. But this domain is a UFD with finitely many units. Therefore, it has an infinite number of prime elements and the infinitude of the set of primes that are sums of squares can be easily proven.

Like above, there are many questions about the infinitude of set of primes and the ring of integers over an algebraic field. We had given some results about the domains $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ where $d \in \mathbb{Z}$. We already know that these domains have an infinite number of prime ideals. The question is: Does there exist a set of primes related with each of these domains? In case of an affirmative answer, can we prove the infinitude of such sets of primes using that correspondence?

With more advanced theory like Algebraic Number Theory we could be able to answer that question. In fact, some results, presented without proof in this work, are related with that topic. Therefore, this work could continue as part of a dissertation.

Bibliography

[1] M.F Atiyah and I.G Mac Donald. *Introduction to Commutative Algebra*. Addison-Wesley, 1969.

[2] D.M. Burton. *Elementary Number Theory*. Mc Graw Hill, 2002.

[3] L.F. Cáceres. *Ultraproducts of sets and ideal theories of commutative rings*. PhD thesis, University of Iowa - Iowa City, 1998.

[4] I.N. Herstein. *Topics in Algebra-second edition*. John Wiley and Sons, 1975.

[5] G. Hiroshi and D.L. McQuillan. On rings with a certain divisibility property. *Michigan Math. J.*, 22:289–299, 1975.

[6] T.W. Hungerford. *Algebra*. Springer-Verlag, 1974.

[7] I. Kaplanski. *Commutative Rings*. Polygonal Publishing House, 1970-1974.

[8] Y.V. Matiyasevich and J.P. Jones. Proof of recursive unsolvability of Hilbert's Tenth Problem. *The American Mathematical Monthly*, 8:689–709, 1991.

[9] W. Narkiewicz. *Polynomial Mappings*. Springer, 1995.

[10] J.A. Vélez. El décimo problema de Hilbert. Technical report, Department of Mathematics, National University of Colombia, December 2001.